IBM QRadar Advisor with Watson

本「サービス記述書」は「クラウド・サービス」について規定するものです。該当する注文関連文書には、お客様の発注に関する価格の詳細情報および追加の詳細情報が記載されています。

1. クラウド・サービス

IBM QRadar Advisor with Watson は、コグニティブ分析を QRadar Security Platform まで拡張して、お客様およびセキュリティー・アナリストが脅威を調査して対応できるようにします。また、Watson for Cyber Security の知識に関するコーパスを活用して、非構造化データ (とりわけ、セキュリティー Web サイト、ブログ、および研究論文を含みます。) を利用し、お客様環境のセキュリティー・インシデントに関連付けます。そうすることにより、隠れた脅威を発見し、洞察を自動化して対応および意思決定を実現できるように手助けします。QRadar Advisor with Watson により、セキュリティー・アナリストは、セキュリティー・オフェンスを Watson へ送信して脅威の発見を実行し、数十万もの非構造化データ・ソースや構造化データ・ソースの知識ベースを使用し、元のセキュリティー・オフェンスに関連する脅威エンティティーにマッピングしなおします (悪意のあるファイル、疑わしい IP アドレス、非認識エンティティー、およびそれらの関係など)。これは、セキュリティー・オフェンスが既知のマルウェア攻撃に関連するものかどうかを判断する際に特に有益です。その場合、Watson は、いくつかある洞察の中で特に、悪用されたマルウェア、悪用された脆弱性、その脅威の範囲 (影響を及ぼす可能性のある追加のエンドポイントを含みます。) に関するバックグラウンドを提供します。

1.1 オファリング

お客様は、利用可能な以下のオファリングから選択することができます。

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson では、お客様が、ローカルのオンプレミス環境またはクラウドのいずれかにアクティブな IBM QRadar の導入を行い、お客様がその機能にアクセスできるように当該導入上に「クラウド・サービス」のイネーブリング・ソフトウェアをインストール済みである必要があります。「クラウド・サービス」が「毎秒イベント数」単位で使用許諾されている場合、「クラウド・サービス」には、お客様が「クラウド・サービス」に送信できるセキュリティー・オフェンスの照会数に関する制限 (お客様が資格を有する「毎秒 100 イベント」ごとに 1 日当たり照会 1.5 件 (直近の照会に切り上げ) の割合) が含まれています。「クラウド・サービス」が「管理対象仮想サーバー (MVS)」単位で使用許諾されている場合、「クラウド・サービス」には、お客様が「クラウド・サービス」に送信できるセキュリティー・オフェンスの照会数に関する制限 (お客様が資格を有する 100 MVS ごとに 1 日当たり照会 15 件の割合) が含まれています。当該制限を超えて送信された照会は優先順位が下がり、当日中は「クラウド・サービス」で処理されない場合があります。

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise は、通常、毎秒 25 万イベント以上の大規模なセキュリティー・オペレーション・センター (SOC) への導入に最も適しています。お客様は、「クラウド・サービス」の機能にアクセスできるように、お客様が個別に取得し、導入した IBM QRadar に「クラウド・サービス」のイネーブリング・ソフトウェアをインストールする必要があります。IBM QRadar Advisor with Watson – Enterprise は、お客様が導入した IBM QRadar の規模とは無関係な「インスタンス」ベースの課金単位に基づいて提供されます。お客様は、任意の時点でのキューの照会が 25 件に制限されます。

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack は、QRadar Advisor with Watson を初めて使用するユーザーを対象にしています。本「クラウド・サービス」は、上述の第 1.1.1 項に記載された QRadar Advisor with Watson の全機能を備えています。ただし、お客様が QRadar Advisor with Watson を初めて購入する際にのみ提供され、更新されることはありません。

1.2 オプション・サービス

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment は、社内のテスト環境への「クラウド・サービス」の導入を希望するお客様向けであり、非実稼働のテストのみを目的として使用することができます。IBM QRadar Advisor with Watson – Test Environment を補完するものとして、実稼働レベルの「クラウド・サービス」に対するサブスクリプションが必要になります。

1.3 アクセラレーション・サービス

1.3.1 IBM QRadar Advisor with Watson Advanced Services

このリモートから提供されるサブスクリプション・サービスでは、IBM は、1 年間に最大 5 日間、以下の任意のコンサルティング・サービスをお客様に提供します。

- お客様の SOC プロセスの評価 (調査またはインシデント対応プロセスを含みます)。
- 参照セットの対応の再評価。
- 大規模攻撃に対する自動分析の調整。
- ユース・ケースの開発。
- QRadar Advisor with Watson を組み込む SOC プロセスの変更に関する推奨事項の提供。
- QRadar Advisor with Watson のデータを理解し、お客様の既存のプロセスに組み込むための、最も効率的な方法に関するガイダンスの提供。
- 関連する QRadar Advisor with Watson 対象に関する知識移転の実行。

注: お客様が導入した QRadar のステータスに基づき、以下のアクティビティーが本サービスに組み込まれることがあります。

- お客様が導入した QRadar に対するヘルス・チェックの実行。
- 既に導入された QRadar に対する追加チューニングの実施。
- お客様が導入した QRadar に新たなログ・ソースを追加する際の支援。

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

本セットアップ・サービスはリモートから提供され、40 時間のプロフェッショナル・サービスが含まれます。このプロフェッショナル・サービスは、すべての時間 (該当する場合) が使用されたかどうかに関係なく、別途記載のない限り、購入から 90 日後に失効します。サービスには、キックオフ電話会議のスケジュールを設定する指定された IBM Engagement Manager が含まれます。

IBM は、以下の一部または全部を実施します。

- お客様の SOC プロセスの評価 (調査またはインシデント対応プロセスを含みます)。
- お客様の環境への QRadar Advisor with Watson の実装。
  - QRadar Advisor with Watson のインストール。
  - 一元化されたプロパティーの QRadar Advisor with Watson へのマッピング。
  - 参照セットの対応の実装。
  - 大規模攻撃に対する自動分析の調整。
  - ユース・ケースのガイダンス。
  - QRadar Advisor with Watson を組み込む SOC プロセスの変更に関する推奨事項の提供。

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

このセットアップ・サービスは、1 秒あたりのイベント (EPS) が 5,000 件未満のお客様向けに設計されています。

このリモートから提供されるサービスでは、IBM は、90 日以内に最大 16 時間、以下の任意のコンサルティング・サービス (またはそれらの組み合わせ) をお客様に提供します。

- QRadar Advisor with Watson のインストール。
- QRadar Advisor with Watson の権限管理。
- QRadar Advisor with Watson の構成。以下が含まれる可能性があります。
  - セキュア・プロキシー・サーバーの構成。
  - X-Force Exchange の資格情報の送信。
  - 許可されたサービス・トークンの作成。
  - 分析結果を保管するための保存ポリシーの構成。
  - カスタム・イベント・プロパティーのマッピング。
  - リファレンス・セットのエクスポート。
  - 脅威インテリジェンスのマッピング。
  - 資産 ID の構成。
  - 使用状況の最適化。
- 自動的なオフェンス調査と結果 (少なくとも 1 つのユース・ケースのショーケース)。
- 関係グラフによる洞察の探求。

2. データ処理およびデータ保護に関するデータ・シート

IBM のデータ処理補足契約書 (http://ibm.com/dpa に公開。「DPA」) のほか、以下のリンクの「データ処理およびデータ保護に関するデータ・シート」 (データ・シートまたは 「DPA 別表」) にも、「クラウド・サービス」およびそのオプション (処理対象の「コンテンツ」の種類、対象となる処理活動、データ保護機能、および「コンテンツ」の保存および返却についての仕様に関連) に関する追加的なデータ保護情報が記載されています。DPA は、i) EU 一般データ保護規則 (EU/2016/679) (GDPR)、または ii) http://ibm.com/dpa/dpl に記載されているその他のデータ保護法が適用される場合に、その適用範囲に限り、「コンテンツ」に含まれる個人データに適用されます。

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206

3. サービス・レベルおよびテクニカル・サポート

3.1 サービス・レベル・アグリーメント

IBM は、以下の可用性のサービス・レベル・アグリーメント (以下「SLA」といいます。) をお客様に提供します。IBM は、下表のとおり、「クラウド・サービス」の累積的な可用性に基づき、適用しうる最大の補償を適用します。「可用性」は、契約月における分単位の総時間数から、契約月における「サービス・ダウン」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。「サービス・ダウン」の定義、請求のプロセス、サービスの可用性の問題に関して IBM に連絡する方法については、IBM の「クラウド・サービス」のサポート・ハンドブック (https://www.ibm.com/software/support/saas_support_overview.html) に掲載されています。

可用性	クレジット (月額サブスクリプション料金のパーセント*)
99.9% 未満	2%
99.0% 未満	5%
95.0% 未満	10%

*サブスクリプション料金は、請求対象月に関して約定した料金です。

3.2 テクニカル・サポート

「クラウド・サービス」のテクニカル・サポート (サポート窓口の連絡先情報、重大度レベル、サポート利用可能時間、応答時間、その他のサポート情報およびサポート・プロセスなど) を参照するには、IBM サポート・ガイド (https://www.ibm.com/support/home/pages/support-guide/) の「クラウド・サービス」を選択します。

4. 料金

4.1 課金単位

「クラウド・サービス」の課金単位は、「個別契約書」に記載されます。

以下の課金単位が本「クラウド・サービス」に適用されます。

- 「1 秒あたりのイベント」(EPS) は、「クラウド・サービス」が処理する特定のイベント、または「クラウド・サービス」の利用に関連する特定のイベントが、1 回発生することをいいます。本「クラウド・サービス」において、「1 秒当たりのイベント」は、お客様が導入した IBM QRadar によって収集および処理されるイベントの数をいいます。
- 「インスタンス」は、「クラウド・サービス」の特定の構成への各アクセスを意味します。
- 「エンゲージメント」とは、「クラウド・サービス」に関するプロフェッショナル・サービスまたはトレーニング・サービスです。
- 「管理対象仮想サーバー (MVS)」は、「クラウド・サービス」で管理される、要求されたプロシージャー、コマンド、またはアプリケーションを実行する処理装置、メモリー、入出力機能で構成されます。

5. 追加条件

2019 年 1 月 1 日よりも前に締結されるクラウド・サービス契約書 (または同等のクラウド基本契約) については、https://www.ibm.com/acs に掲載されている条件を適用します。

5.1 イネーブリング・ソフトウェア

「クラウド・サービス」には以下の「イネーブリング・ソフトウェア」が含まれます。

- IBM QRadar with Watson アプリケーション (https://exchange.xforce.ibmcloud.com/hub)

5.2 クラウド・サービスの合法的利用

「クラウド・サービス」は、お客様のセキュリティー環境およびデータの改善についてお客様を支援するように設計されています。「クラウド・サービス」の利用は、さまざまな法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。「クラウド・サービス」は、合法的目的かつ合法的方法による場合にのみ利用可能です。お客様は、適用される法律、規則、および方針に従って「クラウド・サービス」を利用することに同意し、それらを遵守する一切の責任を負うものとします。お客様は、「クラウド・サービス」の合法的な利用に必要なすべての同意、許可、またはライセンスを取得するか、取得済みであることを表明します。

6. オーバーライド条件

6.1 データの利用

両当事者間の「クラウド・サービス」基本条件の「コンテンツおよびデータ保護」項にいかなる矛盾する規定があっても、以下の条件が優先します。IBM は、お客様の「クラウド・サービス」の利用によって生まれるお客様の「コンテンツ」に固有のものである結果 (以下「洞察」といいます。) や、お客様を特定できる結果を利用したり開示したりしません。ただし、IBM は、「クラウド・サービス」を改善する目的で「クラウド・サービス」の一部として、「コンテンツ」、および「コンテンツ」に由来するその他の情報 (「洞察」を除きます。) を使用します。IBM は、脅威の検知および保護の目的で「コンテンツ」に組み込まれた脅威 ID およびその他のセキュリティー情報も共有できます。